ABSTRACT OF THE DISCLOSURE

Methods and systems for enhancing the security of data during input and output on a client computer system are provided to prevent attempts by unauthorized code to access, intercept, and/or modify data. Example embodiments provide a plurality of obfuscation techniques and security enhanced drivers that use these obfuscation techniques to prohibit unauthorized viewing/receiving of valid data. When the drivers are used together with the various obfuscation techniques, the security enhanced drivers provide mechanisms for "scheduling" the content of the storage areas used to store the data so that valid data is not available to unauthorized recipients. When unauthorized recipients attempt to access the "data," they perceive or receive obfuscated data. The obfuscation techniques described include "copy-in," "replace and restore," and "in-place replacement" de-obfuscation/re-obfuscation techniques. In one embodiment, a security enhanced display driver, a security enhanced mouse driver, a security enhanced keyboard driver, and a security enhanced audio driver are provided. To complement the security enhancements, the methods and systems also provide for a watchdog mechanism to ensure that the driver is functioning as it should be and various user interface techniques for denoting security on a display device.